REMARKS

Reconsideration of this application is respectfully requested. Currently, claims 1-31 and 33-36 are pending in this application. By this Amendment, dependent claims 19, 25 and 35 have been amended to correct their respective dependencies, and claim 32 has been canceled.

The rejection of claims 1-4, 8-10, 12-15, 22-24, 31-34 and 36 under 35 U.S.C. §103 as allegedly being made "obvious" based on Kim '361 in view of Masuda '432 and further in view of Nielson '327 is respectfully traversed.

In order to establish a *prima facie* case of obviousness, all of the claim limitations must be taught or suggested by the prior art. The three-way combination of Kim, Masuda and Nielson fails to teach or suggest all of the claim limitations. For example, the combination fails to teach or suggest "analyzing means arranged to analyze the traffic log data as a function of a predetermined traffic characteristic criterion corresponding to malicious electronic message traffic to identify electronic messages that satisfy the traffic characteristic criterion," as required by independent claim 1 and its dependents. Similar comments apply to independent claims 23 and 36. The combination also fails to teach or suggest "analyzing the traffic log data as a function of a specified traffic characteristic criterion corresponding to malicious electronic message traffic to identify those electronic messages that satisfy the criterion," as required by independent claim 12 and its dependents. Similar comments apply to independent claim 31 and its dependents.

Page 4 of the Office Action admits the following regarding the combination of Kim and Masuda (i.e., "modified Kim"): "The modified Kim fails to teach analyzing means arranged to

analyze the traffic log data as a function of a predetermined traffic characteristic criterion corresponding to malicious electronic message traffic to identify electronic messages that satisfy the traffic characteristic criterion."

Contrary to the further allegations of the Office Action, Nielson fails to resolve the above-described deficiencies of the Kim/Masuda combination (i.e., "modified Kim"). In particular, like Kim and Masuda, Nielson also fails to disclose "analyzing means arranged to analyze the traffic log data as a function of a predetermined traffic characteristic criterion corresponding to malicious electronic message traffic to identify electronic messages that satisfy the traffic characteristic criterion," as required by independent claim 1 for example and/or "analyzing the traffic log data as a function of a specified traffic characteristic criterion corresponding to malicious electronic message traffic to identify those electronic messages that satisfy the criterion," as required by independent claim 12 for example.

In particular, Nielson fails to teach or suggest analyzing traffic log data, let alone analyzing the traffic log data as a function of predetermined traffic characteristic criterion corresponding to malicious electronic message traffic. Instead of malicious electronic message traffic, Nielson is concerned with filtering junk e-mail. Even if junk e-mail were considered to be a form of malicious electronic message traffic, Nielson fails to teach or suggest that this junk e-mail is identified on the basis of an analysis of traffic log data. Instead, a junk e-mail message is identified in Nielson by one recipient opening and analyzing the message itself. However, analyzing a suspicious message itself is precisely what example embodiments of the present invention seek to reduce the need to do, as explained at page 9, line 8 *et seq.* of the present

specification. That portion of the specification explains that the approaches, such as those disclosed in Nielson, which involve the viewing of e-mails themselves are reactive. That is, by the time a virus or junk has been identified, it may have already caused harm or annoyance.

In more detail, Nielson discloses presenting an e-mail message to a trusted recipient. That trusted recipient must read and review the e-mail message to classify it as being a junk e-mail or not. If the trusted recipient (or suitable number of additional trusted recipients) classifies the reviewed e-mail message as being a junk e-mail, Nielson's methodology prevents the presentation of that e-mail (now classified as junk e-email) to other users who have not yet viewed it. Thus, Nielson's system reduces the exposure of junk e-mail messages to other users. However, Nielson's method still requires at least one trusted recipient to carefully read and review the message in order to classify it as a junk e-mail. As noted above, such an approach is reactive insofar as it still requires at least one user to review the e-mail in order to classify it. Any potential harm and/or annoyance may have already been caused by the time that e-mail is classified as a junk e-mail or even upon opening by the first trusted recipient in order to classify it.

The invention of claims 1 and 12 (among others) requires that traffic log data is analyzed in accordance with a predetermined traffic characteristic criterion corresponding to malicious electronic message traffic. Analyzing traffic log data provides an advantage over modified Kim and Nielson in that the need to scan individual messages (or read individual messages) is reduced, thereby leading to a quicker and more processor-efficient method of protection. Again, Nielson's methodology requires that an initial trusted user read that individual message to

classify it as being junk e-mail, so that others might be spared from viewing the junk e-mail. However, a trusted recipient reviewing a received e-mail message to classify it as a junk e-mail fails to teach or suggest analyzing traffic log data. Moreover, Nielson's system requiring a trusted recipient to read and classify a received e-mail message as a junk e-mail certainly does not teach or suggest analyzing traffic log data as a function of a predetermined traffic characteristic criterion corresponding to malicious electronic message traffic.

The traffic log data recited by independent claim 1 or 12 is generated or received based on an at least one traffic characteristic using data derived from *the handling of **plural** electronic messages*. Instead, Nielson's method involves a trusted recipient reading and classifying the message itself. That is, analysis is performed on the message itself in order to determine that it is junk e-mail, rather than being based on data derived from the handling of ***plural*** electronic messages as claimed. This difference reinforces the fact that Nielson's manual review and classification by a trusted recipient fails to teach or suggest analyzing traffic log data, let alone analyzing traffic log data as a function of predetermined traffic characteristic criterion corresponding to malicious electronic message traffic. Accordingly, even if Nielson were combined with modified Kim, the three-way combination would not have taught or suggested all of the claim limitations. In short, Nielson fails to resolve the deficiencies of modified Kim.

Fig. 6 (discussed by col. 9, lines 13-20 -- specifically identified by the Office Action) of Nielson merely discloses a database keeping a record of the number of trusted group members who have classified a particular e-mail message as a junk e-mail. When the value of the number of the trusted group reaches or specifies a value, an e-mail is considered to be a junk e-mail. As

described above, the manual reading and classification of an e-mail as a junk e-mail by one or more trusted recipients in Nielson fails to teach or suggest analyzing traffic log data, let alone analyzing traffic log data as a function of a predetermined traffic characteristic criterion corresponding to malicious electronic message traffic. Even further, the traffic log data is generated or received based on at least one traffic characteristic using data derived the handling of *plural* electronic messages, rather than the review and classification of a single message itself (as in Nielson).

Like the final Office Action, the Advisory Action mailed July 31, 2009 makes reference to col. 9, lines 13-20 of Nielson. Col. 9, lines 13-20 of Nielson states the following:

> Each record 600 in the User's Junk E-mail database contains a "Junk E-mail Characteristics" field 601 and a "Last Date" field 603. The contents of the "Junk E-mail Characteristics" field 601 is associated with a set of text strings. The attributes of the set of text strings associated with this field 601 are described below. The "Last Date" field 603 contains data that represents the calendar date when the record 600 was last used or updated.

With reference to col. 9, lines 13-20, the Advisory Action alleges "Nielson further teaches analyzing the traffic log data as a function of a specified traffic characteristic criterion corresponding to malicious electronic message traffic to identify those electronic messages that satisfy the driterion (sic)." However, this cited passage of Nielson does not teach what the Advisory Action alleges it does. The rest of the Nielsen disclosure is equally lacking in the relevant teaching.

Nielsen addresses the problem of junk email (and not malicious email) while avoiding the possible censorship of a single human moderator or the deficiencies of using filters. The Nielsen

method presents an e-mail message to a trusted human recipient who classifies the message as junk or not (which requires the trusted recipient to open the email). After a sufficient number of trusted individuals have classified a given message as junk, the message is not presented to other users and should also be deleted from the email system.

The Nielsen system does not provide a mechanism generally to classify or characterize email traffic as junk or not: the system is only effective to control the actual emails that are classified as junk by the trusted human recipients of the mail. This approach is clearly unsuited for identifying malicious emails – that is emails containing malicious code – because it requires (multiple) trusted users to open the offending emails in order to apply their classification on which the system relies. Not only does Nielsen fail to teach or suggest a method of dealing with malicious emails, but no skilled person would consider taking any of the Nielsen teaching for application to the handling of malicious emails.

Only two tests are applied by Nielsen's Trusted Group Servers in determining whether an unknown message is the same as a message which has been characterized as junk mail by a trusted user (and hence something which is junk and which should be deleted). The first test is to compare the message ID fields of the two messages (column 10, lines 46 -49). As stated at the foot of column 1, the message ID field contains a unique machine readable identifier "that uniquely identifies each message." The second test requires both message ID fields to be empty (because otherwise they can only have failed the first test by being different – which necessarily means that the two messages are NOT the same message) and that both the originator and subject data of the two messages are the same and that 80% or more of the words in the first five strings

of the body text of each message are the same. If all these points match, then the unknown message is determined to be the one that the trusted user labeled as junk. Finally, if the characteristics do not match, then the unknown message has not been determined to be that labeled as junk by the trusted user – and hence no decision can be made about the unknown message based on any findings of the trusted user.

No mention is made in Nielsen of any log data, nor does identification of filtering of junk mail depend in any way upon log file data.

The rejection of claims 5-7 and 16-18 under 35 U.S.C. §103 as allegedly being made "obvious" based on Kim/Masuda in further view of Toyoshima '349 is also respectfully traversed.

Applicant notes that claims 5-7 and 16-18 depend directly or indirectly from independent base claims 1 and 12, respectively. However, in contrast to the rejection of base independent claims 1 and 12, the rejection of dependent claims 5-7 and 16-18 do not rely on Nielson. As admitted by page 4 of the Office Action, the Kim/Masuda combination (i.e., "modified Kim") fails to teach analyzing the traffic log data as a function of a predetermined traffic characteristic criterion corresponding to malicious electronic message traffic to identify electronic messages that satisfy the traffic characteristic criterion. Toyoshima clearly fails to resolve these admitted deficiencies of modified Kim. Again, the rejection of claims 5-7 and 16-18 do not rely on Nielson, even though the Office Action explicitly relies on Nielson to resolve this admitted deficiency of modified Kim in parent claims 1 and 12. The ground of rejection of Kim/Masuda and Toyoshima therefore appears to be deficient on its face.

The rejection of claims 11, 19 and 35 under 35 U.S.C. §103 as allegedly being made "obvious" based on Kim/Masuda in further view of Tarbotton '830 is also respectfully traversed.

Claims 11, 19 and 35 depend from base independent claims 1, 12 and 23, respectively. Unlike the rejection of claims 1, 12 and 23, the rejection of claims 11, 19 and 35 do not rely on Nielson at all. As discussed above, the combination of Kim and Masuda (i.e., "modified Kim") admittedly fails to teach or suggest all of the limitations required by base independent claims 1, 12 and 23. Tarbotton fails to resolve these admitted deficiencies of modified Kim. As discussed above, Nielson also fails to resolve these deficiencies. Insofar as the rejection of claims 11, 19 and 35 do not rely on Nielson, these rejections appear to be deficient on their face.

The rejection of claim 20 under 35 U.S.C. §103 as allegedly being made "obvious" based on Kim in view of Toyoshima '349 and further in view of Nielson is also respectfully traversed.

The combination of Kim/Nielson and Toyoshima fails to teach or suggest "analyzing the received traffic log data as a function of a specified traffic characteristic criterion corresponding to malicious electronic message traffic to identify those electronic messages that satisfy the criterion," as required by independent claim 20 and its dependents.

The rejection of claim 21 under 35 U.S.C. §103 as allegedly being made "obvious" based on Kim/Toyoshima in further view of Tarbotton '830 is respectfully traversed.

Once again, the Office Action fails to address the earlier admitted deficiency of Kim with respect to the requirement of claim 21 (via its parent claim 20) of receiving traffic log data defining at least one message traffic characteristic, etc., and analyzing such traffic log data as a function of specified traffic characteristic criterion corresponding to malicious electronic

message traffic, etc. That is, unlike the rejection of base independent claim 20, the rejection of claim 21 (which depends from claim 20) does not rely on Nielson. The rejection of claim 21 thus appears to be deficient on its face.

The rejection of claims 25-30 under 35 U.S.C. §103 as allegedly being made "obvious" based on Kim/Masuda in further view of Khanna '604 is also respectfully traversed.

Once again, the admitted fundamental deficiencies of Kim/Masuda have been noted above for base independent claim 1. Khanna fails to resolve those admitted deficiencies. Nielson is not relied upon in the rejection of claims 25-30, even though Nielson is relied upon in the rejection of base independent claim 1. Insofar as the rejection of claims 25-30 does not rely on Nielson, the rejection of claims 25-30 appears to be erroneous on its face.

Conclusion:

Accordingly, this entire application is now believed to be in condition for allowance, and a formal notice to that effect is earnestly solicited.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: _____
Raymond Y. Mah
Reg. No. 41,426

RYM:dmw
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100